



Malware de firewall



INTRODUCCIÓN

Las amenazas de malware pueden estar presentes, y las organizaciones pueden usar varias técnicas y servicios para mitigar estas amenazas (por ejemplo, firewalls, software antivirus y prácticas recomendadas de control de usuarios). Este laboratorio se enfoca en técnicas de contramedidas usando un firewall.

OBJETIVOS

- Actualizar un firewall de red de AWS
- Crear un grupo de reglas de firewall
- Verificar y probar que el acceso a los sitios maliciosos esté bloqueado



TAREA 1

En esta tarea, inicia sesión en la instancia TestInstance de EC2 que se preconfiguró durante la preparación del laboratorio. Desde ahí, emite un comando wget a los archivos del actor malicioso que el equipo de TI le proporcionó para confirmar la accesibilidad.

- Desde la página de la consola de Vocareum, seleccione el botón de detalles de AWS.
- Junto a TestInstanceURL, hay un enlace. Copie y pegue el enlace en un nuevo laboratorio en su navegador web.
- Cambiar directorios y ver el directorio de trabajo actual.
- En este entorno de laboratorio protegido, ingrese el código y presione Intro para descargar parte del malware.
- En este entorno de laboratorio protegido, ingrese el código y presione Intro para descargar el resto del malware.

```
ID de sesión: user3386630-Joseph_Julios-      ID de instancia: i-01d6d585c707ae921      Terminar
e2tuw7gwrwferdx45gv74aaq

sh-4.2$ cd ~
sh-4.2$ pwd
/home/ssm-user
sh-4.2$ wget http://malware.wicar.org/data/js_crypto_miner.html
--2024-08-21 06:20:42-- http://malware.wicar.org/data/js_crypto_miner.html
Resolving malware.wicar.org (malware.wicar.org)... 208.94.116.246, 2607:fff8:80:6::6a08
Connecting to malware.wicar.org (malware.wicar.org)|208.94.116.246|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 366 [text/html]
Saving to: 'js_crypto_miner.html'

100%[=====>] 366      --.-K/s   in 0s

2024-08-21 06:20:42 (51.4 MB/s) - 'js_crypto_miner.html' saved [366/366]

sh-4.2$ wget http://malware.wicar.org/data/java_jre17_exec.html
--2024-08-21 06:20:51-- http://malware.wicar.org/data/java_jre17_exec.html
Resolving malware.wicar.org (malware.wicar.org)... 208.94.116.246, 2607:fff8:80:6::6a08
Connecting to malware.wicar.org (malware.wicar.org)|208.94.116.246|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 129 [text/html]
Saving to: 'java_jre17_exec.html'

100%[=====>] 129      --.-K/s   in 0s

2024-08-21 06:20:51 (20.6 MB/s) - 'java_jre17_exec.html' saved [129/129]

sh-4.2$
```



- Ver los archivos descargados.

ID de sesión: user3386630=Joseph_Julios-
e2tuw7gwrrwferrdx45gv74aqq

ID de instancia: i-01d6d585c707ae921

```
sh-4.2$ ls
java_jre17_exec.html  js_crypto_miner.html
sh-4.2$
```



TAREA 2

En esta tarea, inspeccionará el firewall de AWS Network Firewall que se configuró durante la preparación del laboratorio. Actualizar este firewall es la prioridad principal que le asignó AnyCompany como el nuevo ingeniero de seguridad.

- En la consola de administración de AWS, ingrese VPC en la barra de búsqueda y luego seleccione VPC.
- En el panel de navegación izquierdo, en NETWORK FIREWALL, seleccione Firewalls

The screenshot displays the AWS Management Console interface for the 'Network Firewall: firewalls' section. The left-hand navigation pane is expanded, showing the 'Network Firewall' category with 'Firewalls' selected. The main content area, titled 'Firewalls', shows a table with one entry: 'LabFirewall'. The table has columns for 'Nombre', 'Estado', and 'Estado de sincronización de la configuración'. The 'LabFirewall' entry is in the 'Listo' (Ready) state and is 'Sincronizado' (Synchronized). The bottom status bar indicates '0 firewall seleccionado'.

- Seleccione LabFirewall y lea los tres pasos en la sección Overview.



- En el Paso 2: Configurar la política de firewall, seleccione el enlace de LabFirewallPolicy para abrir la política asociada.
- En la sección Stateless default actions, seleccione Edit.
- Para Stateless default actions (Acciones predeterminadas sin estado), configure las siguientes opciones.

The screenshot shows the AWS Management Console interface for configuring a Network Firewall Policy. The left sidebar contains navigation links for various services, including Security, Firewall DNS, Network Firewall, and Red privada virtual (VPN). The main content area displays the 'LabFirewallPolicy' configuration page. A modal window titled 'Acciones predeterminadas sin estado' is open, allowing users to configure default actions for rules without state. The modal includes options for handling fragmented packets, selecting actions for rules without state, and publishing metrics. The 'Guardar' (Save) button is highlighted in orange.

- Seleccione Save (Guardar).



TAREA 3

En esta tarea, creará un grupo de reglas de firewall de red con reglas que bloquean el acceso a las URL maliciosas. Luego adjuntará esta regla a su política de firewall.

- En el panel de navegación izquierdo, en NETWORK FIREWALL, seleccione Network Firewall Rule Groups.
- Seleccione Create Network Firewall rule group.
- En la sección Create Network Firewall rule group (Crear grupo de reglas de firewall de red), configure las opciones de Rule group type y Stateful rule group.
- En la sección Suricata compatible IPS rules, ingrese el código en el cuadro de texto.

The screenshot shows the AWS Management Console interface for creating a Network Firewall Rule Group. The left sidebar contains a navigation menu with steps: Paso 1: Elegir tipo de grupo de reglas, Paso 2: Describir grupo de reglas, Paso 3: Configurar reglas, Paso 4 - opcional: Configuración de los ajustes avanzados, Paso 5 - opcional: Agregar etiquetas, and Paso 6: Revisar y crear. The main content area is titled 'Revisar y crear' and shows three steps: Paso 1: Tipo de grupo de reglas, Paso 2: Grupo de reglas, and Paso 3: Reglas. Paso 1 shows 'Tipo de grupo de reglas' as 'Con estado', 'Opción de grupo de reglas con estado' as 'Suricata compatible rule string', and 'Orden de las reglas' as 'strict'. Paso 2 shows 'Detalles del grupo de reglas' with 'Nombre' as 'StatefulRuleGroup', 'Descripción' as '-', and 'Capacidad' as '100'. Paso 3 shows 'Variables de regla (0)' with a table with columns 'Nombre' and 'Tipo'.

Nombre	Tipo
--------	------



- Seleccione Create stateful rule group.

Panel de VPC

Vista global de EC2

Filter by VPC

Nube virtual privada

- Sus VPC
- Subredes
- Tablas de enrutamiento
- Puertas de enlace de Internet
- Puerta de enlace de Internet de solo salida
- Gateways de operador
- Conjuntos de opciones de DHCP
- Direcciones IP elásticas
- Listas de prefijos administradas
- Puntos de conexión
- Servicios de punto de conexión
- Gateways NAT
- Interconexiones

Seguridad

- ACL de red
- Grupos de seguridad

Ha creado correctamente grupo de reglas StatefulRuleGroup.

VPC > Grupos de reglas de Network Firewall

Grupos de reglas

Un grupo de reglas es un conjunto reutilizable de reglas de firewall para inspeccionar y filtrar el tráfico de la red. Puede usar grupos de reglas sin estado o con estado a fin de configurar los criterios de inspección del tráfico para sus políticas de firewall. Puede crear sus propios grupos de reglas o utilizar grupos de reglas administrados por vendedores de AWS Marketplace.

Sus grupos de reglas | Grupos de reglas administrados por AWS

Agregar grupos de reglas a la política

La siguiente tabla enumera todos los grupos de reglas.

Sus grupos de reglas (1)

Eliminar | Crear grupo de reglas

Buscar recursos por nombre o valor

<input type="checkbox"/>	Nombre	Tipo
<input type="checkbox"/>	StatefulRuleGroup	Stateful

0 grupos de reglas seleccionados



TAREA 4

En esta tarea, adjuntará el grupo de reglas de firewall de red que creó al firewall de red.

- En el panel de navegación izquierdo, en NETWORK FIREWALL, seleccione Firewalls.
- Seleccione LabFirewall.
- En Step 2, seleccione la lista desplegable Add rule groups y luego seleccione Add from existing stateful rule groups.
- Seleccione la casilla para StatefulRuleGroup y luego seleccione Add stateful rule group.

The screenshot shows the AWS Management Console interface for configuring a Network Firewall. The breadcrumb navigation at the top indicates the path: VPC > Políticas de firewall de Network Firewall > LabFirewallPolicy. The main heading is 'Agregar grupos de reglas con estado no administradas' (Add unmanaged stateful rule groups). Below this, a message states: 'Una política de firewall se puede asociar a varios firewalls. La modificación de una política de firewall afecta a todos los firewalls que hacen referencia a ella. Para utilizar grupos de reglas administrados por usted, consulte las integraciones de la red de socios de AWS (APN).' (A firewall policy can be associated with multiple firewalls. Modifying a firewall policy affects all firewalls that reference it. To use rule groups managed by you, see AWS Partner Network integrations). The 'Grupo de reglas con estado (1/1)' (Stateful rule groups (1/1)) section contains a search bar and a table with one row: 'StatefulRuleGroup'. The 'Nombre' (Name) checkbox is checked. At the bottom, there are 'Cancelar' (Cancel) and 'Agregar un grupo de reglas con estado' (Add stateful rule group) buttons.



- Desplácese hasta la sección Stateful rule groups para ver el grupo de reglas que se agregó correctamente.

Panel de VPC

Ha actualizado correctamente política de firewall LabFirewallPolicy.

No hay grupos de reglas sin estado

Elija Agregar grupos de reglas para agregar grupos de reglas sin estado a la política.

Orden de evaluación de reglas con estado y acciones predeterminadas

La forma en que se ordenan las reglas con estado para su evaluación.

Orden de las reglas	Acciones predeterminadas
Orden de acción	-

Grupos de reglas con estado (1)

Nombre	Capacidad	¿Está administrado?	¿Poner en marcha en modo de alerta?
StatefulRuleGroup	100	No	No disponible

Unidades de capacidad consumidas por los grupos de reglas sin estado

El total de unidades de capacidad consumidas por los grupos de reglas sin estado no puede ser superior a 30 000.

0/30,000

Unidades de capacidad consumidas por los grupos de reglas con estado

El total de unidades de capacidad consumidas por los grupos de reglas con estado no puede superar 30,000.

100/30,000

© 2024, Amazon Web Services, Inc. o sus filiales. Privacidad Términos Preferencias de cookies



TAREA 5

En esta tarea, volverá a iniciar sesión en TestInstance para probar que el firewall de red bloquee correctamente los intentos de acceder a los archivos del sitio web malicioso.

- En la consola de administración de AWS, ingrese EC2 en la barra de búsqueda y luego seleccione EC2.
- En el panel de navegación izquierdo, elija Instances.
- Seleccione la casilla junto a TestInstance, y luego seleccione Connect.
- Cambiar directorios y ver el directorio de trabajo actual.

ID de sesión: user3386630=Joseph_Julios-nkqnvvdnb5cnadt4bxzkccs4uq

ID de instancia: i-01d6d585c707ae921

```
sh-4.2$ cd ~
sh-4.2$ pwd
/home/ssm-user
sh-4.2$ █
```

- Para intentar acceder al primer archivo malicioso, ejecute el siguiente comando wget.

ID de sesión: user3386630=Joseph_Julios-nkqnvvdnb5cnadt4bxzkccs4uq

ID de instancia: i-01d6d585c707ae921

```
sh-4.2$ wget http://malware.wicar.org/data/js_crypto_miner.html
--2024-08-21 06:53:58-- http://malware.wicar.org/data/js_crypto_miner.html
Resolving malware.wicar.org (malware.wicar.org)... 208.94.116.246, 2607:ff18:80:6::6a08
Connecting to malware.wicar.org (malware.wicar.org)|208.94.116.246|:80... connected.
HTTP request sent, awaiting response...
```



- Presione Ctrl+c para detener el comando.
- Para probar las otras URL maliciosas, ejecute el siguiente comando.

ID de sesión: user3386630=Joseph_Julios-
nkqnvvdnb5cnadt4bxzkccs4uq

ID de instancia: i-01d6d585c707ae921

```
sh-4.2$ wget http://malware.wicar.org/data/java_jre17_exec.html
--2024-08-21 06:55:06-- http://malware.wicar.org/data/java_jre17_exec.html
Resolving malware.wicar.org (malware.wicar.org)... 208.94.116.246, 2607:ff18:80:6::6a08
Connecting to malware.wicar.org (malware.wicar.org)|208.94.116.246|:80... connected.
HTTP request sent, awaiting response...
```

- A continuación, para eliminar los archivos de malware de prueba, ejecute el siguiente comando.
- Confirmar que los archivos se eliminaron.

ID de sesión: user3386630=Joseph_Julios-
nkqnvvdnb5cnadt4bxzkccs4uq

ID de instancia: i-01d6d585c707ae921

```
sh-4.2$ rm java_jre17_exec.html js_crypto_miner.html
sh-4.2$ ls
sh-4.2$
```